



E-Authentication Implementation Workshop

Moving Towards Production

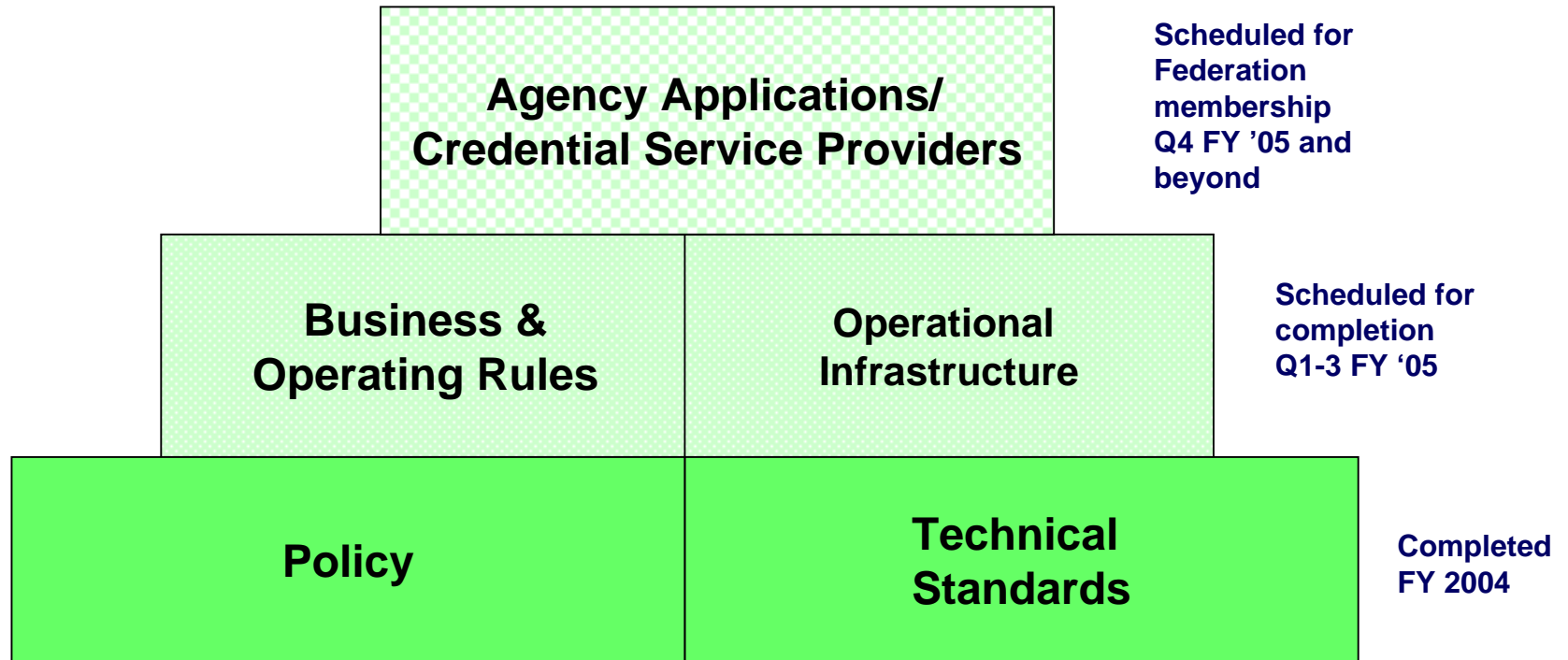
April 12 & 14, 2005



Agenda

- ◆ Building the E-Authentication Federation
- ◆ E-Authentication Policy Foundation
- ◆ Agency Application Deployment
 - Process
 - Milestones and Deliverables
 - Roles and Responsibilities
- ◆ How to Work with the E-Authentication PMO
- ◆ E-Authentication User Group

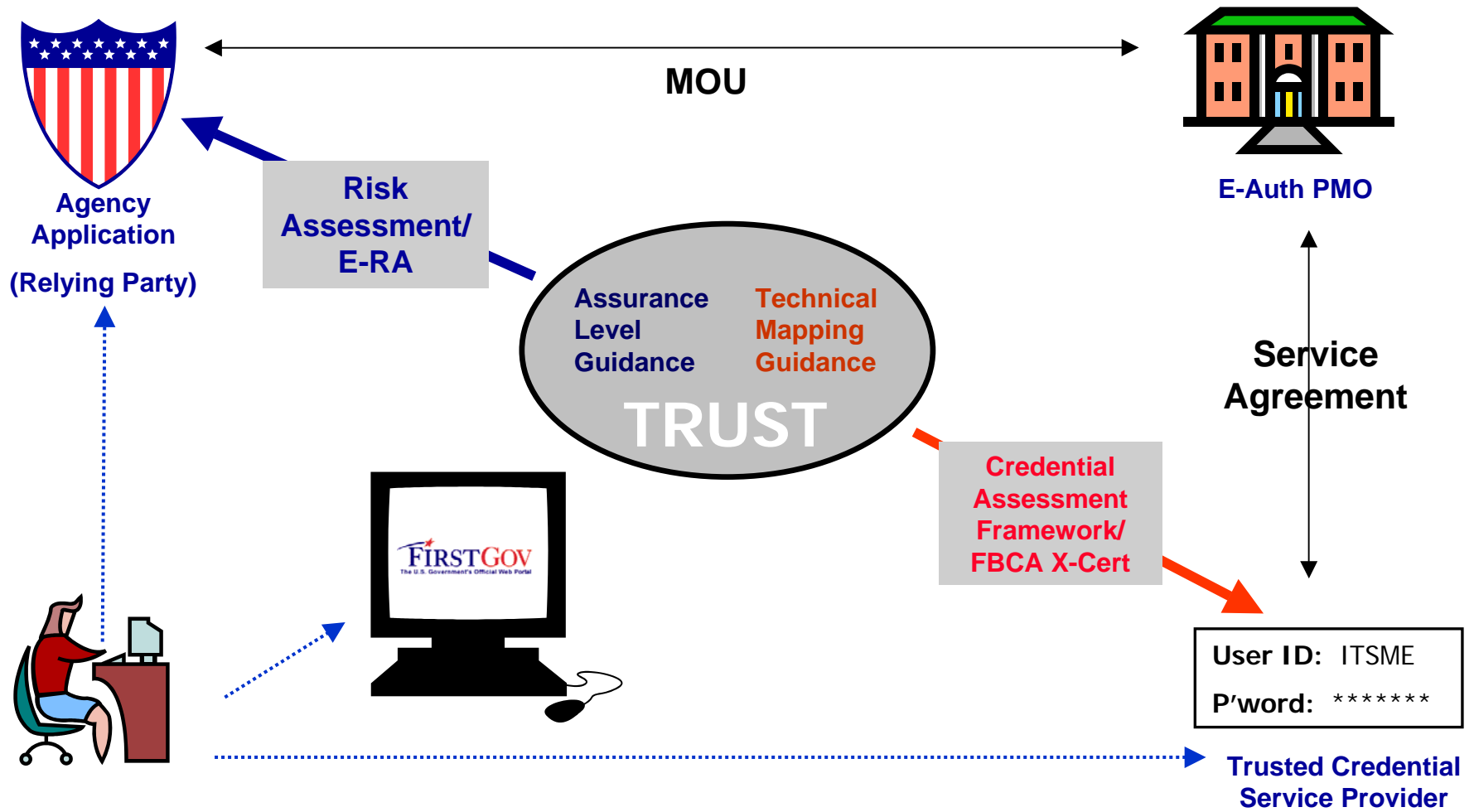
Building the E-Authentication Federation



The Policy Foundation is in Place

- ◆ Policy infrastructure enables *real* business and trust— because it can be universally leveraged and accepted
- ◆ Policy framework key to E-Authentication Federation context and cohesiveness
- ◆ Policy framework necessary for:
 - Technical architecture and interoperability
 - Evaluation of credential service providers
 - Determination of assurance level requirements
- ◆ Tools:
 - OMB M-04-04
 - E-Authentication Risk and Requirements Assessment (E-RA)
 - NIST SP 800-63
 - Credential Assessment Framework (CAF)

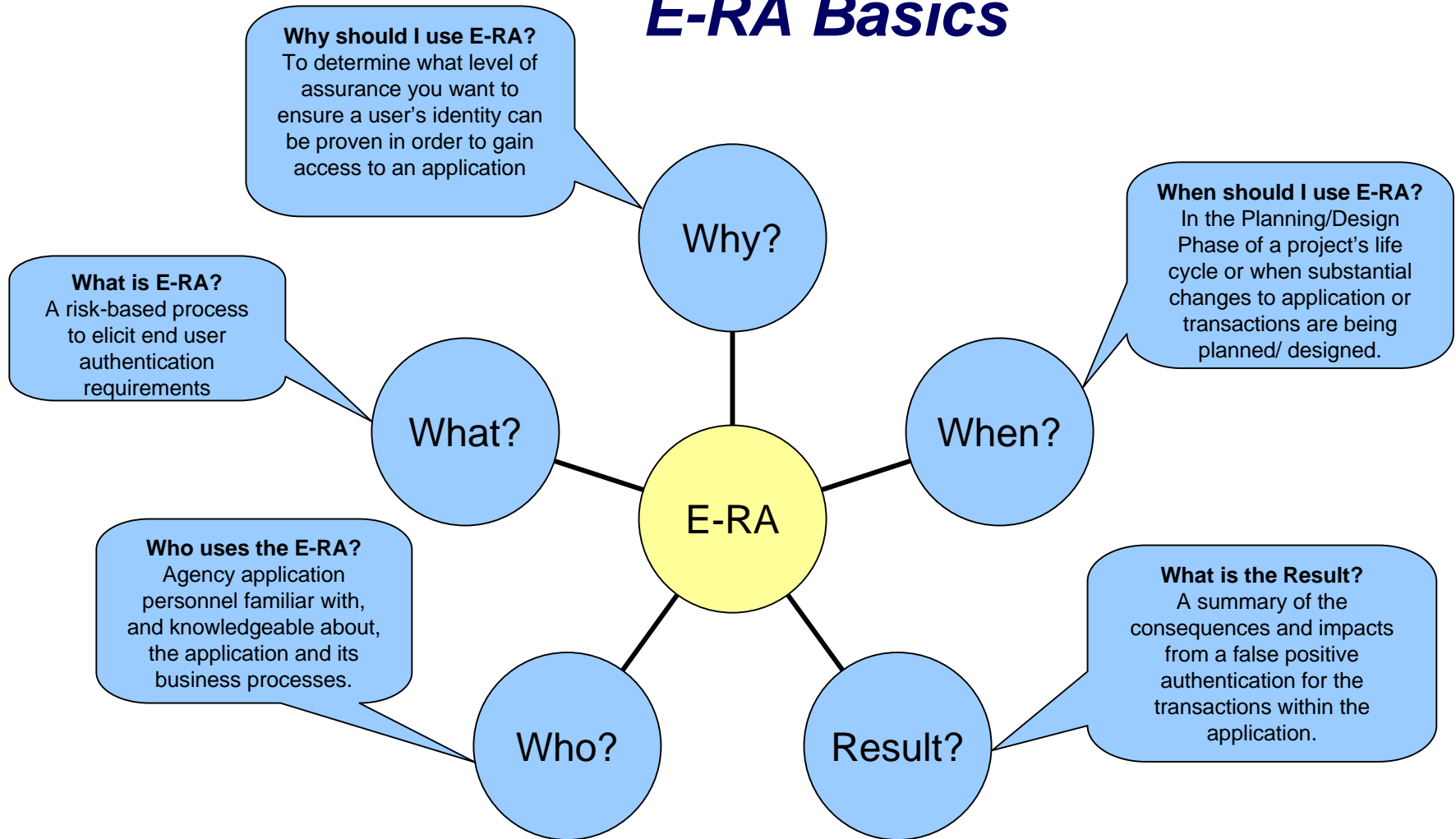
Putting Policy into Practice



What is the e-Risk Assessment?

- ◆ The E-RA approach:
 - Identifies key user roles and transactions within the application
 - Organizes consequences of false positive authentication and impacts to the agency
 - Aids in mapping the application to a set of pre-defined authentication criteria by aligning each transaction to a consequence level

E-RA Basics



Applications: Process

- ◆ Process outlined in project plan template
- ◆ Can align with dept/agency system life cycle
- ◆ Defined standard milestones and deliverables to use for status tracking

Milestones and Deliverables

- ◆ Kickoff Meeting Conducted
- ◆ Initial Project Plan Prepared
- ◆ OMB-Defined Assurance Level Determined
- ◆ System Requirements Specification Delivered
- ◆ Updated Project Plan Prepared
- ◆ System Design Document Delivered

Milestones and Deliverables (continued)

- ◆ Lab Prerequisites Checklist Completed
- ◆ Successful Acceptance Testing
- ◆ Completed Boarding Checklist

- ◆ Application Performs Live E-Authentication-Enabled Transactions!!!

Roles and Responsibilities: Agency/Department/Application

- ◆ Comply with E-Authentication policies and specifications
- ◆ Name a Project Manager and conduct kickoff meeting
- ◆ Prepare and execute project plan
- ◆ Provide status reports and meet at least semi-monthly
- ◆ Acquire and deploy software from approved vendors
- ◆ Process acceptable credentials from trusted CSPs

Roles and Responsibilities: E-Authentication PMO

- ◆ Provide E-Authentication expertise, guidance, and documentation
- ◆ Facilitate kickoff meetings
- ◆ Provide input into the project plan

How to Work with the E-Authentication PMO

◆ Agency Relationship Managers (ARM)

- Main point of contact
- One ARM is assigned per department/agency
- List included in binder

◆ Technical Subject Matter Expert (SME)

- Primary SME is point of contact to discuss architecture and technical issues
- Supported by additional SMEs as needed

◆ Interoperability Lab

- Performs acceptance testing
- ARM/SME schedules 2-3 months in advance

Application Status Tracking

- ◆ Provide status updates to ARMs on semi-monthly or agreed upon basis
 - High-level project description
 - Milestones agreed to in MOU plus any additional milestones
 - Project issues, risks, and mitigation strategies
- ◆ Discuss project plan in regularly held meetings between ARM, SME and application representatives
- ◆ Identify and track issue resolution

E-Authentication User Group

- ◆ Provides a forum and networking opportunity for Federation participants
- ◆ Initial meeting in March
- ◆ Membership
- ◆ Topics addressed:
 - Architecture change proposals
 - Federation practices and operating and rules
 - Risk Assessments and Credential Assessment Framework
- ◆ Next meeting planned for May

Links to Collateral

- ◆ **The E-Authentication Technical Architecture:**
 - <http://cio.gov/eauthentication/TechSuite.htm>
- ◆ **The E-Authentication Handbook for Federal Agencies:**
 - <http://cio.gov/eauthentication/documents/GOVhandbook.pdf>
- ◆ **E-Authentication Guidance for Federal Agencies (M-04-04):**
 - <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>
- ◆ **E-Authentication Risk and Requirements Assessment (E-RA):**
 - <http://cio.gov/eauthentication/era.htm>
- ◆ **Electronic Authentication Guideline (NIST SP 800-63):**
 - http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf
- ◆ **E-Authentication Credential Assessment Suite:**
 - <http://cio.gov/eauthentication/CredSuite.htm>
- ◆ **E-Authentication Cookbook:**
 - <http://cio.gov/eauthentication/documents/Cookbook.pdf>

Questions????

For More Information



Judy Cohen

703-872-8622

judith.cohen@gsa.gov

Myisha Frazier-McElveen

703-872-8626

myisha.frazier.mcelveen@gsa.gov

Thomas Peters

703-872-8585

thomas.peters@gsa.gov

Websites

<http://cio.gov/eauthentication>

<http://cio.gov/fpkipa>